

Quantum Computing on Lattices using Global Two-Qubit Gates

G. Ivanyos*

Computer and Automation Research Institute,
Hungarian Academy of Sciences,
H-1518 Budapest, P.O. Box 63., Hungary.

S. Massar†

Laboratoire d'Information Quantique and QUIC, C.P. 165/59,
Av. F. D. Roosevelt 50, B-1050 Bruxelles, Belgium

A. B. Nagy‡

Budapest University of Technology and Economics,
H-1521 Budapest, P.O. Box 91., Hungary.

We study the computation power of lattices composed of two dimensional systems (qubits) on which translationally invariant global two-qubit gates can be performed. We show that if a specific set of 6 global two qubit gates can be performed, and if the initial state of the lattice can be suitably chosen, then a quantum computer can be efficiently simulated.

PACS numbers: 03.67.Lx

I. INTRODUCTION

Building a computer that operates coherently at the quantum level may revolutionise the way we carry out computations. Indeed it is believed that such quantum computers are much more powerful than their classical analogues. For instance it seems that factoring can be carried out exponentially faster on a quantum computer than on a classical computer. For this reason much work is being devoted to developing physical systems in which computation can be carried out at the quantum level.

A very attractive systems in which to implement quantum information processing are atomic lattices. Indeed the method for realising such lattices suggested in [1] has been demonstrated in [2], and lattices comprising more than 10^5 atoms have been realised. A method for carrying out interactions between neutral atoms suggested in [3] has been demonstrated in [4]. This method realises a global two-qubit gate which in a few steps can entangle all the lattice, leading to cluster states[5]. Finally coherent transport of atoms over many lattice spacings has been demonstrated in [6] which implies that the global two-qubit gates can be realised between atoms located many lattice spacings away.

On the other hand atomic lattices are affected with a fundamental difficulty. Namely it is very difficult in these systems to address individually each atom in the lattice. Rather one is limited to the global operations mentioned above. Thus whereas atomic lattices seem well suited to carry out simulations of translationally invariant physical systems[7], it is not as clear how to use them to implement a universal quantum computer.

Here we address the question of the computational power of atomic lattices. That is, to what extent can a quantum computer be efficiently realised using atomic lattices?

We shall consider a perfect lattice, i.e. a lattice with exactly one atom per site. We shall suppose that the only gates which are available are global one-qubit gates and global two-qubit gates. We will suppose that these gates can be performed perfectly. We shall also take each atom to have an internal Hilbert space of dimension 2, i.e. a qubit. These restrictions strongly limit the operations that can be carried out and the core of our result consists of showing how to overcome these constraint. Finally we shall suppose that the initial state of the lattice breaks slightly the translational symmetry in a specific way. Namely we shall suppose that all the atoms are initially in the state $|0\rangle$ except two specific atoms that are in the state $|1\rangle$. Our main result is to show that in this situation it is possible to efficiently simulate a quantum computer.

We note that experiments so far involving atomic lattices have only used qubits (as we do), but also have only implemented a single global two-qubit Hamiltonian which in the notation below is $|01\rangle\langle 01|^{(d)}$. On the other hand the

*Electronic address: Gabor.Ivanyos@sztaki.hu

†Electronic address: smassar@ulb.ac.be

‡Electronic address: nagy@math.bme.hu

result we report here requires two different global two-qubit gates and global one-qubit gates. Whether or not the Hamiltonian $|01\rangle\langle 01|^{(d)}$ and arbitrary global one-qubit gates are enough to simulate a quantum computer is an open question. The results obtained here may provide an avenue for tackling this problem. We expect they will also be of interest in other contexts as they provide a non trivial way of implementing a quantum computer in a system where limited sets of gates are realisable.

The question of the computational power of atomic lattices has recently been studied in a number of works. For instance the proposals of [8] and [9] are based on the concept of a “marker qubit” which is circulated through the lattice. And [10] uses as ingredient imperfections in the lattice. The latter work has been extended in [11] to perfect lattices and translationaly invariant initial states. The techniques used in these works are very different from the ones presented here. Essential differences concern for instance the size of the Hilbert space of each atom, the initial state, and the way local gates between logical qubits are implemented using the global gates.

Finally it may be interesting to note that the present work was motivated by a numerical study of the computational power of atomic lattices. In this numerical investigation we allowed all global one-qubit gates and a single global two-qubit gate on qubit pairs of distance 1 on a lattice consisting of n qubits on a circle. We considered the action of these global gates on the eigenspaces of the cyclic shift operator in the Hilbert space of the states of the n qubits corresponding to the eigenvalue 1. (As the shift operator commutes with the global gates, all of its eigenspaces are invariant under the action of global gates.) Using the computational algebra system GAP [12], we obtained that for $n = 3, \dots, 7$ qubits, the restriction of the Hamiltonians of global gates to the eigenspace generate the whole unitary Lie algebra. That is, at least up to 7 qubits, the above global gates form a universal set of gates on the eigenspace. If this holds for every n (as we conjecture), global one-qubit gates and a single global two-qubit gate on a cyclic lattice consisting of n qubits can implement arbitrary unitaries on a Hilbert space of size roughly $n - O(\log_2 n)$ qubits.

A possible reason for the universality we found is that the global two-qubit gate considered has almost as many eigenvalues as possible. But this means that in some sense this gate acts “chaotically”. Therefore the model is probably not very useful in the sense that it does not seem to allow one to define a qubit structure on the eigenspace in a natural way. For this reason we turned to the model described above which uses more two-qubit gates, which allows a qubit structure to be defined, and which is amenable to analytic treatment. It is this analysis we report here.

II. GLOBAL TWO-QUBIT GATES

We begin by giving a precise definition of global two-qubit gates.

Let D be a subset of an abelian group G where $|D| = n$. The Hilbert space of the pure states of the n qubits is \mathbb{C}^{2^n} . The elements of the standard basis are indexed by the functions $D \rightarrow \{0, 1\}$. For a function $a : D \rightarrow \{0, 1\}$ the corresponding basis element is denoted by $|a\rangle$. If $p \in D$ we also write a_p for the value $a(p) \in \{0, 1\}$.

For a 2-qubit operation or $2^2 \times 2^2$ matrix M and a pair of elements $p, q \in D$, $M^{(p,q)}$ denotes the n -qubit operation which acts as M on the pair of qubits at positions p and q :

$$M_{a,b}^{(p,q)} = \begin{cases} M_{(a_p, a_q), (b_p, b_q)} & \text{if } a_s = b_s \text{ for every } s \in D \setminus \{p, q\}, \\ 0 & \text{otherwise,} \end{cases}$$

or, in the bra-ket notation

$$\langle a | M^{(p,q)} | b \rangle = \begin{cases} \langle a_p a_q | M | b_p b_q \rangle & \text{if } a_s = b_s \text{ for every } s \in D \setminus \{p, q\}, \\ 0 & \text{otherwise,} \end{cases}$$

We introduce a *weight function* $W : D \times D \rightarrow \mathbb{R}$ on the pairs of D . This function corresponds to the fact that the global qubit gate can act with different strength on different pairs of atoms in the lattice. We could take W to be constant, thereby respecting the translation invariance. For a two-qubit matrix M and a vector $d \in G$ the *global operation* $M^{(d)}$ is the sum of all copies of M acting on pairs of qubits having difference d , weighted by W :

$$M^{(d)} = \sum_{\substack{p, q \in D \\ p - q = d}} W(p, q) M^{(p,q)}.$$

A *global 2-qubit Hamiltonian* is a matrix of the form $H^{(d)}$ where H is an Hermitian (i.e., self-adjoint) 2-qubit operation and a *global 2-qubit gate* is an operation of the form $\exp(-iH^{(d)})$ where $H^{(d)}$ is a global two-qubit Hamiltonian.

III. AN EFFICIENT ENCODING

The key to our approach is to use a subset $P \subset D$ of the qubits as logical qubits. All the qubits in P should initially be in a known state, for instance all in the state $|0\rangle$. The rest of the qubits will be set initially to the $|0\rangle$ state except for two particular qubits r and r' which are set to $|1\rangle$. The qubits in $D \setminus (P \cup \{r, r'\})$ play a separator role in the computation and are always brought back to $|0\rangle$ after each elementary logical gate, whereas the qubits r and r' are always brought back to $|1\rangle$ after each logical gate. The qubits r and r' serve as reference points in our method. Intuitively, they are used to "locate" logical qubits and help to "extract" local operations at the right places from global ones. The subset P and r, r' obey some geometrical constraints which we now describe.

1. If $p \in P, s \in \{r, r'\}, q, q' \in P \cup \{r, r'\}$ such that $q - q' = p - s$ then $q = p$ and $q' = s$. That is for every $p \in P$, both $p - r$ and $p - r'$ occur exactly once as a difference of a pair of points from $P \cup \{r, r'\}$.
2. If $q, q' \in P \cup \{r, r'\}$ such that $q - q' = r - r'$ then $q = r$ and $q' = r'$. That is $r - r'$ occurs exactly once as a difference of a pair of points from $P \cup \{r, r'\}$.
3. For every $p \in P$ there exists no pair $q, q' \in P \cup \{r, r'\}$ such that $p - r + p - r' = q - q'$.

Examples. It is not difficult to find groups G and sets $P, \{r, r'\}$ that satisfy these constraints.

- An l dimensional lattice of size m in each direction: $G = \mathbb{Z}^l, D = \{0, \dots, m-1\}^l, P = \{p = (p_1, \dots, p_l) \in D \mid \sum_{i=1}^l p_i \equiv 0 \pmod{6}\} \setminus \{0\}, r = (1, 0, \dots, 0), r' = (2, 0, \dots, 0)$. Here $|P| = |D|/6 - 1$, i.e., roughly every sixth element of D belongs to P .
- A circle of size $n = 6k$: $D = G = \mathbb{Z}_n, P = \{p \in G \mid p \equiv 0 \pmod{6}\} \setminus \{0\}, r = 1, r' = 2$. In this example $|P|$ is again $|D|/6 - 1$.
- An l dimensional lattice of size $m = 3j + 1$ in each direction. $G = \mathbb{Z}^l, D = \{0, \dots, m-1\}^l, P = \{p = (p_1, \dots, p_l) \in D \mid 2j + 1 \leq p_1 \leq 3j\}, r = (0, \dots, 0), r' = (j, 0, \dots, 0)$. Here $|P| = jm^{l-1} = \frac{m-1}{3}m^{l-1} \approx |D|/3$.

It is not difficult to generalise these examples or combine them in different ways.

We say that a function $a : D \rightarrow \{0, 1\}^n$ is *admissible* if $a_r = a_{r'} = 1$ and $a_p = 0$ for every other $p \in D \setminus P$. Let $k = |P|$. Then functions $\{1, \dots, k\} \rightarrow \{0, 1\}$ can be identified with the admissible functions in a natural way therefore admissible functions can encode k qubits.

We can now state our main theorem:

Theorem 1 *Assume that for every pair $q \neq q' \in P \cup \{r, r'\}$, we have $W(q, q') \neq 0$. Let $w = \max\{|W(q, q')| : q \neq q' \in D\} / \min\{|W(q, q')| : q \neq q' \in P \cup \{r, r'\}\}$. Assume further that for every pair $p \neq p' \in P$, the following global two-qubit gates can be implemented for any t and $\delta \in \{0, 1\}$:*

$$\exp\left(-t\iota(|11\rangle\langle 11|)^{(p-r)}\right), \quad \exp\left(-t\iota(|11\rangle\langle 11|)^{(p-r')}\right), \quad (1)$$

$$\exp\left(-t(|1\delta\rangle\langle 0\delta| - |0\delta\rangle\langle 1\delta|)^{(p-p')}\right), \quad \exp\left(-t\iota(|1\delta\rangle\langle 0\delta| + |0\delta\rangle\langle 1\delta|)^{(p-p')}\right). \quad (2)$$

Then on the Hilbert space of the admissible functions $|P|$ -qubit quantum computations can be efficiently simulated using global gates of type (1) and (2). Here by efficiency we mean that the complexity of the simulation, measured in the number of global two-qubit gates used, is polynomial in w, n and the complexity of the original computation.

An upper bound on the efficiency, i.e. on the degree of the polynomial, can be obtained from the proofs of theorems 1 and 6. This upper bound is probably far from optimal.

Section V is devoted to the proof of this result. However we shall first show that one can achieve the same result as stated in Theorem 1 by using global one-qubit gates and fewer global two qubit-gates.

IV. USING FEWER GLOBAL TWO-QUBIT GATES

The gates eq. (1) are the global controlled phase gates. It is interesting to note that the global gates eq. (2) can be thought of as generating global Controlled-NOT gates. Indeed the two-qubit Hamiltonians appearing in these gates are

$$\sigma_x \otimes |\delta\rangle\langle\delta| \quad , \quad \sigma_y \otimes |\delta\rangle\langle\delta| .$$

which exponentiated for time $\pi/2$ yield

$$\exp\left(-i\frac{\pi}{2}(|1\delta\rangle\langle0\delta| + |0\delta\rangle\langle1\delta|)\right) = (-i(|1\rangle\langle0| + |0\rangle\langle1|) \otimes |\delta\rangle\langle\delta|) ;$$

and similarly for the other gates in eq. (2), but in different bases. Note however that the interpretation as a C-NOT is not valid for the global gate, because the Hamiltonians acting on the different pairs of qubits do not commute.

Let us now show that if one can realise global one-qubit gates, then the four global two-qubits eq. (2) can all be implemented once a single one can be implemented. To see this we will denote a global one-qubit gate as

$$u^{global} = \prod_{p \in D} u^{(p)}$$

where $u^{(p)}$ is the unitary transformation that acts as u on the qubit at position p only:

$$\langle a|u^{(p)}|b\rangle = \begin{cases} \langle a_p|u|b_p\rangle & \text{if } a_s = b_s \text{ for every } s \in D \setminus \{p\}, \\ 0 & \text{otherwise.} \end{cases}$$

We then have

$$\begin{aligned} u^{global} e^{-iH^{(d)}} u^{global\dagger} &= e^{-iu^{global} H^{(d)} u^{global\dagger}} \\ &= \exp \left[-i \sum_{\substack{p, q \in D \\ p - q = d}} W(p, q) u^{(p)} u^{(q)} H^{(p, q)} u^{(p)\dagger} u^{(q)\dagger} \right] \end{aligned} \quad (3)$$

Using this expression it is easy to see that the four global 2 qubit-gates appearing eq. (2) are equivalent if one can implement the global one-qubit gates σ_x^{global} and $(1/\sqrt{2} + i\sigma_z/\sqrt{2})^{global}$.

Note that the class of global two-qubit operations that can be implemented when a single global two-qubit operation and arbitrary global one-qubit operations can be implemented is larger than the class given in eq. (3), see [13].

V. PROOF OF MAIN THEOREM

Our aim is to show how local gates between two qubits $p, p' \in P$ can be efficiently implemented by sequences of global gates (1) and (2). We will first study how this can be done at the level of Hamiltonians by commuting $A^{(p-r)} = (|11\rangle\langle11|)^{(p-r)}$, $A^{(p-r')} = (|11\rangle\langle11|)^{(p-r')}$ and the Hamiltonians of the global gates in (2). These results on commutation of Hamiltonians will then imply the results for the implementation of two qubit gates, ie. for unitary operations.

For $a, b : D \rightarrow \{0, 1\}$ the elementary matrix with zeros at every position except for a, b where the entry is one is denoted by $E_{a,b}$:

$$E_{a,b} = |a\rangle\langle b|.$$

For $a : D \rightarrow \{0, 1\}$ and $p \in D$ we denote by $\text{del}_p(a)$ the function that can be obtained by zeroing the bit of a at position p :

$$\text{del}_p(a)_q = \begin{cases} a_q & \text{if } q \neq p, \\ 0 & \text{if } q = p. \end{cases}$$

Our first step will be to investigate how the commutations act on the elementary matrix $E_{a, \text{del}_p(a)}$.

Recall that A is the two-qubit operation $|11\rangle\langle 11|$. Its matrix is a diagonal matrix with entry one at position corresponding to $|11\rangle$ and zero elsewhere:

$$A_{a,b} = \langle a|A|b\rangle = \begin{cases} 1 & \text{if } a = b = 11, \\ 0 & \text{otherwise.} \end{cases}$$

Thus if $0 \neq d \in G$ then $A^{(d)}$ is the diagonal matrix where the element at the position corresponding to a is just the sum of the weights of the $1 - 1$ pairs in a having difference d :

$$A_{a,a}^{(d)} = \langle a|A^{(d)}|a\rangle = \sum_{\substack{p, q \in D \\ p - q = d}} W(p, q) \langle a|A^{(p,q)}|a\rangle = \sum_{\substack{p, q \in D \\ p - q = d \\ a_p = a_q = 1}} W(p, q).$$

As a consequence, if a is a function from D to $\{0, 1\}$ and $q \in D$ with $a_q = 1$, then we have the following formula:

$$[A^{(d)}, E_{a,\text{del}_q(a)}] = (a_{q-d}W(q, q-d) + a_{q+d}W(q+d, q))E_{a,\text{del}_q(a)}. \quad (4)$$

(Here, in order to simplify notation, we assume that $W(l, l') = 0$ if $l \notin D$ or $l' \notin D$). Indeed,

$$\begin{aligned} [A^{(d)}, E_{a,\text{del}_q(a)}] &= A^{(d)}|a\rangle\langle \text{del}_q(a)| - |a\rangle\langle \text{del}_q(a)|A^{(d)} \\ &= \sum_{\substack{p', q' \in D \\ p' - q' = d \\ a_{p'} = a_{q'} = 1}} W(p', q')|a\rangle\langle \text{del}_q(a)| - \sum_{\substack{p', q' \in D \\ p' - q' = d \\ \text{del}_q(a)_{p'} = \text{del}_q(a)_{q'} = 1}} W(p', q')|a\rangle\langle \text{del}_q(a)|. \end{aligned}$$

All the terms of the second sum appear also in the first one and the possible terms of the first sum missing from the second one are $W(q, q-d)|a\rangle\langle \text{del}_q(a)|$ (if $a_{q-d} = 1$) and $W(q+d, q)|a\rangle\langle \text{del}_q(a)|$ (if $a_{q+d} = 1$). This gives (4).

A consequence of (4) is that if a is admissible, $a_q = 1$, $p \in P$ and $s \in \{r, r'\}$ then

$$[A^{(p-s)}, E_{a,\text{del}_q(a)}] = \begin{cases} W(p, s)E_{a,\text{del}_q(a)} & \text{if } q \in \{p, s\} \text{ and } a_p = 1, \\ 0 & \text{otherwise.} \end{cases} \quad (5)$$

Indeed, $q \in P \cup \{r, r'\}$ by admissibility of a . If $a_{q-(p-s)} = 1$ then $q - (p-s) \in P \cup \{r, r'\}$ which implies $q = p$ and $q - (p-s) = s$ by the first constraint on $P \cup \{r, r'\}$. In addition $q + p - s \notin P \cup \{r, r'\}$ and therefore $a_{q+p-s} = 0$ and the coefficient given in (4) is $W(p, s)$. Similarly, $a_{q+p-s} = 1$ is possible if and only if $q = s$ and $p = q + p - s$ and in this case, using once more the first constraint on $P \cup \{r, r'\}$ the coefficient is again $W(p, s)$ since $a_{p-(p-s)}W(p, p - (p-s)) = a_sW(p, s) = W(p, s)$. This discussion proves (5).

On the other hand, if a is not admissible but $\text{del}_q(a)$ is admissible then

$$[A^{(p-s)}, E_{a,\text{del}_q(a)}] = 0, \text{ provided that } \{q - p + s, q + p - s\} \cap (P \cup \{r, r'\}) = \emptyset. \quad (6)$$

This follows from (4) and the fact that all the possible positions where $\text{del}_q(a)$ can be 1 fall in the set $P \cup \{r, r'\}$ (by admissibility of $\text{del}_q(a)$).

These results are the basic ingredients for proving:

Lemma 2 *Assume that a is an admissible function with $a_q = 1$ and $b = \text{del}_q(a)$. Then for every $p \in P$, we have*

$$[A^{(p-r)}, [A^{(p-r')}, E_{a,\text{del}_q(a)}]] = \begin{cases} W(p, r)W(p, r')E_{a,\text{del}_q(a)} & \text{if } q = p \text{ and } a_p = 1, \\ 0 & \text{otherwise.} \end{cases}$$

If a is not admissible but $\text{del}_q(a)$ is admissible then for every $p \in P$,

$$[A^{(p-r)}, [A^{(p-r')}, E_{a,\text{del}_q(a)}]] = 0.$$

Proof. Assume that a is admissible. Then repeated applications of (5) (first for $s = r'$ and then for $s = r$) give that $[A^{(p-r)}, [A^{(p-r')}, E_{a,\text{del}_q(a)}]]$ can be nonzero only if $q \in \{p, r'\} \cap \{p, r\} = \{p\}$, that is $q = p$. On the other hand, again

using (5) twice, it is straightforward to verify that $[A^{(p-r)}, [A^{(p-r')}, E_{a,\text{del}_p(a)}]] = W(p, r)W(p, r')E_{a,\text{del}_p(a)}$. This finishes the proof of the first assertion.

To see the second statement, assume that the commutator is nonzero. Then, by (6), $\{q-p+r', q+p-r'\} \cap (P \cup \{r, r'\}) \neq \emptyset$ and $\{q-p+r, q+p-r\} \cap (P \cup \{r, r'\}) \neq \emptyset$. Assume first that $q-p+r', q-p+r \in P \cup \{r, r'\}$. Then, using $r-r' = (q-p+r) - (q-p+r')$ and the second constraint on $P \cup \{r, r'\}$, we have $r = q-p+r$, $r' = q-p+r'$ and $q = p \in P$. But then if a is not admissible then $\text{del}_q(a)$ is not admissible either, a contradiction. (The case $q+p-r', q+p-r \in P \cup \{r, r'\}$ can be treated in a similar way).

Finally, assume that $q+p-r', q-p+r \in P \cup \{r, r'\}$ (the remaining case can be treated by a symmetric argument). Then $(q+p-r') - (q-p+r) = (p-r) + (p-r')$, which is impossible by the third property of the configuration $P \cup \{r, r'\}$. \square

We will now use lemma 2 to show how commutations of certain global two-qubit operators $B_\delta^{(p-q)}$ with $A^{(p-r)}$ and $A^{(p-r')}$ yields a local two qubit operator. The operators $B_\delta^{(p-q)}$ will be the basic constituents of the Hamiltonians of the global gates in (2). We define $B_\delta = |\delta\rangle\langle 0\delta|$ for $\delta \in \{0, 1\}$, i.e. $B_0 = |10\rangle\langle 00|$ and $B_1 = |11\rangle\langle 01|$. Assume that we take an order of the basis where the first $2^{|P|}$ basis elements correspond to the admissible functions and the rest correspond to the inadmissible functions. The next lemma states that in this order of basis the matrix of $[A^{(p-r)}, [A^{(p-r')}, B_\delta^{(p-q)}]]$ for $p, q \in P$ is block diagonal where the upper left $2^{|P|} \times 2^{|P|}$ block is a scalar multiple of the corresponding block of $B_\delta^{(p,q)}$.

Lemma 3 *Let $p \neq q \in P$, $a, b : D \rightarrow \{0, 1\}$ such that either a or b is admissible. Then*

$$\langle a | [A^{(p-r)}, [A^{(p-r')}, B_\delta^{(p-q)}]] | b \rangle = W(p, q)W(p, r)W(p, r')\langle a | B_\delta^{(p,q)} | b \rangle.$$

In particular if only one of a and b is admissible then

$$\langle a | [A^{(p-r)}, [A^{(p-r')}, B_\delta^{(p-q)}]] | b \rangle = 0.$$

Proof. For every $a, b : D \rightarrow \{0, 1\}$ and for every pair $p' \neq q' \in D$ we have $\langle a | B_\delta^{(p',q')} | b \rangle = 1$ if and only if $a_{p'} = 1$, $b_{p'} = 0$, $a_{q'} = b_{q'} = \delta$, and $a_s = b_s$ for every $s \in D \setminus \{p', q'\}$. Otherwise $\langle a | B_\delta^{(p',q')} | b \rangle = 0$. An equivalent formulation of this is

$$B_\delta^{(p',q')} = \sum_{\substack{a : D \rightarrow \{0, 1\}, \\ a_{p'} = 1, a_{q'} = \delta}} E_{a,\text{del}_{p'}(a)}.$$

From this equality we infer

$$\begin{aligned} B_\delta^{(p-q)} &= \sum_{\substack{p', q' \in D, \\ p' - q' = p - q}} W(p', q') B_\delta^{(p',q')} \\ &= \sum_{\substack{p', q' \in D, \\ p' - q' = p - q}} \sum_{\substack{a : D \rightarrow \{0, 1\}, \\ a_{p'} = 1, a_{q'} = \delta}} W(p', q') E_{a,\text{del}_{p'}(a)} \\ &= \sum_{a : D \rightarrow \{0, 1\}} \sum_{\substack{p', q' \in D, \\ p' - q' = p - q \\ a_{p'} = 1, a_{q'} = \delta}} W(p', q') E_{a,\text{del}_{p'}(a)}. \end{aligned}$$

Using the latter equality, Lemma 2 and the fact that $[A^{(p-r)}, [A^{(p-r')}, E_{a,b}]]$ is always a scalar multiple of $E_{a,b}$, we obtain

$$\langle a | [A^{(p-r)}, [A^{(p-r')}, B_\delta^{(p-q)}]] | b \rangle = \begin{cases} W(p, r)W(p, r')W(p, q) & \text{if } b = \text{del}_p(a), a_p = 1 \text{ and } a_q = \delta, \\ 0 & \text{otherwise,} \end{cases}$$

whenever either a or b is admissible. From this equality the assertions follow as

$$\langle a | B_\delta^{(p,q)} | b \rangle = \begin{cases} 1 & \text{if } b = \text{del}_p(a), a_p = 1 \text{ and } a_q = \delta, \\ 0 & \text{otherwise.} \end{cases}$$

\square

From lemma 3 we easily derive a similar result regarding the block structure of the matrices obtained by commuting the Hamiltonians of the global gates in (2) with the Hamiltonians of the global gates (1). The result can be interpreted as stating that, restricted to the subspace spanned of the admissible states, the commutators coincide (up to a scalar multiple) with the Hamiltonians of the corresponding (local) two-qubit gates acting on the pair of qubits at positions p and q .

Proposition 4 For $\delta \in \{0, 1\}$ let U_δ be any of the Hamiltonians $-(|1\delta\rangle\langle 0\delta| - |0\delta\rangle\langle 1\delta|)$ and $-\iota(|1\delta\rangle\langle 0\delta| + |0\delta\rangle\langle 1\delta|)$. Let $p \neq q \in P$, $a, b : D \rightarrow \{0, 1\}$ such that either a or b is admissible. Then

$$\langle a|[-\iota A^{(p-r)}, [-\iota A^{(p-r')}, U_\delta^{(p-q)}]]|b\rangle = -W(p, q)W(p, r)W(p, r')\langle a|U_\delta^{(p,q)}|b\rangle.$$

Proof. We give the proof only for $U_\delta = -|1\delta\rangle\langle 0\delta| + |0\delta\rangle\langle 1\delta|$, as the calculations for the other case are essentially the same. Observe that $U_\delta = -B_\delta + B_\delta^\dagger$. Hence, using also that the matrices $A^{(p-r)}$ and $A^{(p-r')}$ are self-adjoint,

$$\begin{aligned} [-\iota A^{(p-r)}, [-\iota A^{(p-r')}, U_\delta^{(p-q)}]] &= -[A^{(p-r)}, [A^{(p-r')}, U_\delta^{(p-q)}]] \\ &= [A^{(p-r)}, [A^{(p-r')}, B_\delta^{(p-q)}]] - [A^{(p-r)}, [A^{(p-r')}, B_\delta^{(p-q)\dagger}]] \\ &= [A^{(p-r)}, [A^{(p-r')}, B_\delta^{(p-q)}]] - [A^{(p-r)}, [A^{(p-r')}, B_\delta^{(p-q)}]]^\dagger. \end{aligned}$$

By Lemma 3, this gives

$$\begin{aligned} \langle a|[-\iota A^{(p-r)}, [-\iota A^{(p-r')}, U_\delta^{(p-q)}]]|b\rangle &= W(p, q)W(p, r)W(p, r')\langle a|B_\delta^{(p,q)}|b\rangle - W(p, q)W(p, r)W(p, r')\langle a|B_\delta^{(p,q)\dagger}|b\rangle \\ &= -W(p, q)W(p, r)W(p, r')\langle a|U^{(p,q)}|b\rangle, \end{aligned}$$

whenever either a or b is admissible. \square

This result can be used to show that local gates on pairs of qubits in P can be efficiently simulated using global gates. To prove this we will need some standard facts regarding approximations of unitary operators.

For an operator U on the Hilbert space \mathbb{C}^n we denote by $\|U\|$ the operator norm of U : $\|U\| = \sup_{|x|=1} |Ux|$. Note that $\|AB\| \leq \|A\| \cdot \|B\|$. If $\|A_1\|, \|A_2\|, \|B_1\|, \|B_2\| \leq 1$ then we have

$$\|A_1A_2 - B_1B_2\| = \|(A_1 - B_1)A_2 + B_1(A_2 - B_2)\| \leq \|A_1 - B_1\| \cdot \|A_2\| + \|B_1\| \cdot \|A_2 - B_2\| \leq \|A_1 - B_1\| + \|A_2 - B_2\|.$$

By an easy induction we obtain

$$\|A_1 \cdots A_N - B_1 \cdots B_N\| \leq \sum_{j=1}^N \|A_j - B_j\|, \quad (7)$$

whenever A_1, \dots, A_N and B_1, \dots, B_N are sequences of unitary operators.

Lemma 5 There is an absolute constant $c > 0$, such that

$$\left\| \left(\exp\left(-\frac{\iota}{\sqrt{N}}U^{-1}\right) \cdot \exp\left(-\frac{\iota}{\sqrt{N}}V^{-1}\right) \cdot \exp\left(-\frac{\iota}{\sqrt{N}}U\right) \cdot \exp\left(-\frac{\iota}{\sqrt{N}}V\right) \right)^N - \exp(-\iota U, -\iota V) \right\| < c \cdot M^3 N^{-\frac{1}{2}}$$

for any $N > M^2$, where U and V are Hermitian operators on the Hilbert space \mathbb{C}^n and $M = \max\{\|U\|, \|V\|, 1\}$.

Proof. We use the first three terms in the expansion of $\exp(-t\iota U)$:

$$\exp(-t\iota U) = 1 - t\iota U - \frac{1}{2}t^2U^2 + O(M^3t^3),$$

as $t \rightarrow 0$. The norm of the error term can be indeed upper bounded by

$$\sum_{j=3}^{\infty} \frac{1}{j!} (tM)^j = M^3 t^3 \sum_{j=0}^{\infty} \frac{1}{(j+3)!} (tM)^j < M^3 t^3 \sum_{j=0}^{\infty} \frac{1}{j!} (tM)^j = M^3 t^3 e^{tM} \leq e \cdot M^3 t^3$$

if $t < 1/M$. Doing the same for $\exp(-t\iota V)$, $\exp(t\iota U)$, and $\exp(t\iota V)$ and collecting the terms with exponent greater than 2 we obtain

$$\begin{aligned} & \exp(-t\iota U)^{-1} \cdot \exp(-t\iota V)^{-1} \cdot \exp(-t\iota U) \cdot \exp(-t\iota V) \\ &= (1 + t\iota U - \frac{t^2}{2}U^2)(1 + t\iota V - \frac{t^2}{2}V^2)(1 - t\iota U - \frac{t^2}{2}U^2)(1 - t\iota V - \frac{t^2}{2}V^2) + O(M^3t^3) \\ &= 1 + t^2(VU - UV) + O(M^3t^3) = 1 + t^2[\iota U, \iota V] + O(M^3t^3). \end{aligned}$$

On the other hand, taking just the first two term of the expansion of $\exp([-t\iota U, -t\iota V])$, we obtain $\exp([-t\iota U, -t\iota V]) \approx 1 + t^2[\iota U, \iota V]$, where the norm of the error term can be upper bounded by

$$(2M^2)^2 t^4 e^{4M^2 t^2} \leq 4e^4 \cdot M^4 t^4 \leq 4e^4 M^3 t^3$$

whenever $t < 1/M$. This, and the preceding formula gives

$$\|\exp(-t\iota U^{-1}) \cdot \exp(-t\iota V^{-1}) \cdot \exp(-t\iota U) \cdot \exp(-t\iota V) - \exp[-t\iota U, \exp -t\iota V]\| \leq c \cdot M^3 t^3$$

for $t < 1/M$ with some constant c . Writing $t = 1/\sqrt{N}$ in the latter inequality we obtain the asserted result using formula (7). \square

Now we are in a position to prove our main technical result from which theorem 1 will easily follow.

Theorem 6 *Assume that for every $p' \neq q' \in D$ and $p'' \neq q'' \in P \cup \{r, r'\}$ we have $\frac{|W(p', q')|}{|W(p'', q'')|} \leq w$. Then, for every real $-1 \leq T \leq 1$, for every $p \neq q \in P$, for every $\delta \in \{0, 1\}$, and for every $0 < \epsilon < 1$, operations which act as the two qubit gates*

$$\exp\left(-T(|1\delta\rangle\langle 0\delta| - |0\delta\rangle\langle 1\delta|)^{(p,q)}\right), \quad \exp\left(-T\iota(|1\delta\rangle\langle 0\delta| + |0\delta\rangle\langle 1\delta|)^{(p,q)}\right) \quad (8)$$

on admissible states can be ϵ -approximated by a product of $(nw/\epsilon)^{O(1)}$ global gates of type (1) and (2).

Proof. Let U stand for any of the global Hamiltonians $\iota(|1\delta\rangle\langle 0\delta| - |0\delta\rangle\langle 1\delta|)^{(p,q)}$ and $(|1\delta\rangle\langle 0\delta| + |0\delta\rangle\langle 1\delta|)^{(p,q)}$. Let $V = [1/W(p, r')|11\rangle\langle 11|^{(p-r')}, -\iota T/W(p, q)U]$. Note that for any $p, q \in P$, for any $s \in \{r, r'\}$, $\|-\iota T/W(p, q)U\| \leq 2nw$, $\|1/W(p, s)|11\rangle\langle 11|^{(p-s)}\| \leq nw$, $\|1/W(p, r)|11\rangle\langle 11|^{(p-r)}\| \leq nw$, $\|V\| \leq 4w^2n^2$.

By Proposition 4, we need to approximate the operation $\exp([-t\iota/W(p, r)|11\rangle\langle 11|^{(p-r)}, -\iota V])$. By Lemma 5 this can be done with error at most $\epsilon/2$ using a product of $O(N_2)$ operations which are either global operations of the form $\exp(\pm\iota/(W(p, r)\sqrt{N_2})|11\rangle\langle 11|^{(p-r)})$ or operations of the form $\exp(\pm\iota/\sqrt{N_2}V)$, where $N_2 = O(w^{12}n^{12}/\epsilon^2)$.

Furthermore by formula (7), we obtain an ϵ -approximation if we use $\epsilon/(2N_2)$ -approximations instead of the operators $\exp(\pm\iota\sqrt{N_2}V)$. By Lemma 5 we can $\epsilon/(2N_2)$ -approximate the operators $\exp(\pm\iota\sqrt{N_2}V) = \exp(\pm[-\iota W(p, r')^{-1}N_2^{-1/4}|11\rangle\langle 11|^{(p-r')}, -\iota TW(p, q)^{-1}N_2^{-1/4}U])$ by a product of N_1 global gates where $N_1 = O(w^6n^6N_2^{1/2}\epsilon^{-2}) = O(w^{12}n^{12}\epsilon^{-3})$.

The total number of global gates used in the approximation of the "local" one is $O(N_1N_2) = O(w^{24}n^{24}\epsilon^{-5})$. \square

Lemma 7 *The gates*

$$\exp(-t(|1\delta\rangle\langle 0\delta| - |0\delta\rangle\langle 1\delta|)), \quad \exp(-t\iota(|1\delta\rangle\langle 0\delta| + |0\delta\rangle\langle 1\delta|)). \quad (9)$$

for $\delta \in \{0, 1\}$ and for real numbers $-1 \leq t \leq 1$ form a universal set of two-qubit gates.

Proof. We claim that the following six $2^2 \times 2^2$ matrices generate su_{2^2} as a Lie algebra over \mathbb{R} :

$$\begin{aligned} U &= |11\rangle\langle 01| - |01\rangle\langle 11|, \quad Y = \iota|11\rangle\langle 01| + \iota|01\rangle\langle 11|, \\ T &= |11\rangle\langle 10| - |10\rangle\langle 11|, \quad X = \iota|11\rangle\langle 10| + \iota|10\rangle\langle 11|, \\ V &= |10\rangle\langle 00| - |00\rangle\langle 10|, \quad Z = \iota|10\rangle\langle 00| + \iota|00\rangle\langle 10|. \end{aligned}$$

Indeed, a basis of su_{2^2} can be obtained as

$$\begin{aligned} & T, U, V, X, Y, Z, \\ [V, T] &= |00\rangle\langle 11| - |11\rangle\langle 00|, \quad [T, Z] = \iota|00\rangle\langle 11| + \iota|11\rangle\langle 00|, \\ [T, U] &= |01\rangle\langle 10| - |10\rangle\langle 01|, \quad [Y, T] = \iota|01\rangle\langle 10| + \iota|10\rangle\langle 01|, \\ [[V, T], U] &= |00\rangle\langle 01| - |01\rangle\langle 00|, \quad [[T, Z], U] = \iota|00\rangle\langle 01| + \iota|01\rangle\langle 00|, \\ [U, Y] &= 2\iota(|11\rangle\langle 11| - |01\rangle\langle 01|), \quad [T, X] = 2\iota(|11\rangle\langle 11| - |10\rangle\langle 10|), \quad [V, Z] = 2\iota(|10\rangle\langle 10| - |00\rangle\langle 00|). \end{aligned}$$

From the claim the assertion follows as the matrices U, V, Y , and Z are Hamiltonians of operations of the form (9), while T and X can be obtained from U and Y , respectively, by exchanging the two qubits. \square

We now prove our main theorem:

Proof of Theorem 1. Consider a quantum computation (circuit) on $|P|$ qubits. Because of Lemma 7, we may assume that the circuit is given as a product of ℓ gates of the form (9) acting on qubit pairs in P , i.e., gates given in (8). (The complexity in terms of other, more standard gate set is polynomially related to ℓ .) Let $\epsilon > 0$. By (7), we obtain an ϵ -approximation of the circuit if we use ϵ/ℓ -approximations of the gates. By Theorem 6, the effect of an individual 2-qubit gate on admissible configurations can be approximated with error at most ϵ/ℓ using $O((wn\ell/\epsilon)^k)$ global two-qubit gates of the form (1) and (2) for some constant $k \leq 24$. In view of this, simulation of the entire circuit requires $O(\ell(wn\ell/\epsilon)^k) \leq O((wn\ell/\epsilon)^{k+1})$ global gates. \square

VI. CONCLUSION

In the present work we have considered the computational power of a lattice composed of a two dimensional system (a qubit) at each site. The only gates we used were global two-qubit gates which act in a translationally invariant manner on pairs of qubits. The initial state of the lattice consists of all qubits in the $|0\rangle$ state, except two specific qubits which are in the $|1\rangle$ state. With these ingredients we have shown that it is possible to efficiently simulate a quantum computer. We hope these results will stimulate further work on the computational power of lattice systems.

Preliminary investigations suggest that one can extend the present work in several directions. First of all it should be possible to decrease the number of different types of global two-qubit gates which are used in the simulation. Secondly we have not exploited in the present work the global one-qubit gates. Preliminary work shows that they can be used to simplify some aspects of the simulation.

Acknowledgments: We are grateful to Ignacio Cirac for presenting us the model of global gates, for suggesting the question of equivalence with conventional quantum computers and also for his useful remarks and suggestions. We thank Lajos Rónyai for his helpful suggestions regarding the proofs. We acknowledge financial support by project RESQ IST-2001-37559 of the IST-FET program of the EC, by the Communauté Française de Belgique under grant ARC00/05-251, by the IUAP program of the Belgian government under grant V-18 and by the Hungarian Scientific Research Fund (OTKA) under grants T42706 and T42481.

- [1] D. Jaksch, C. Bruder, J. I. Cirac, C. W. Gardiner, P. Zoller, Phys. Rev. Lett. **81** (1998) 3108
- [2] M. Greiner, O. Mandel, T. Esslinger, T. W. Hänsch, I. Bloch, Nature **415** (2002) 39
- [3] D. Jaksch, H.-J. Briegel, J. I. Cirac, C. W. Gardiner, P. Zoller, Phys. Rev. Lett. **82** (1999) 1975
- [4] O. Mandel, M. Greiner, A. Wildra, T. Rom, T. W. Hänsch, I. Bloch, Nature **425** (2003) 937
- [5] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. 86, 5188 (2001).
- [6] O. Mandel, M. Greiner, A. Wildra, T. Rom, T. W. Hänsch, I. Bloch, Phys. Rev. Lett. **91** (2003) 010407
- [7] E. Jané, G. Vidal, W. Dür, P. Zoller, J. I. Cirac, Quantum Information and Computation, Vol. 3, No. 1, 15-37 (2003)
- [8] T. Calarco, U. Dorner, P. Julienne, C. Williams, P. Zoller, quant-ph/0403197.
- [9] A. Kay, J. K. Pachos, New. J. Phys. 6 (2004) 126
- [10] K. G. H. Vollbrecht, E. Solano, and J. I. Cirac, Phys. Rev. Lett. 93, 220502 (2004)
- [11] K. G. H. Vollbrecht, J. I. Cirac, *Reversible universal quantum computation within translation invariant systems*, quant-ph/0502143
- [12] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4; 2004. (<http://www.gap-system.org>)
- [13] L. Masanes, G. Vidal, J. I. Latorre, quant-ph 0202042